USAISEC
US Army Information Systems Engineering Command
Fort Huachuca, AZ 85613-5300

U.S. ARMY INSTITUTE FOR RESEARCH
IN MANAGEMENT INFORMATION,
COMMUNICATIONS, AND COMPUTER SCIENCES

AIRMICS

Mitre Lad Evaluation

ASQB-GM-91-011

January 1991

AIRMICS
115 O'Keefe Building
Georgia Institute of Technology
Atlanta, GA 30332-0800

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188
Exp. Date: Jun 30, 1986

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS NONE
2a. SECURITY CLASSIFICATION AUTHORITY N/A	3. DISTRIBUTION/AVAILABILITY OF REPORT N/A
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) ASQB-GM-91-011	5. MONITORING ORGANIZATION REPORT NUMBER(S) N/A
6a. NAME OF PERFORMING ORGANIZATION AIRMICS 6b. OFFICE SYMBOL (*If applicable*) ASQB-GM	7a. NAME OF MONITORING ORGANIZATION N/A
6c. ADDRESS (City, State, and Zip Code) 115 O'Keefe Bldg. Georgia Institute of Technology Atlanta, Ga 30332-0800	7b. ADDRESS (*City, State, and ZIP Code*) N/A
8b. NAME OF FUNDING/SPONSORING ORGANIZATION AIRMICS 8b. OFFICE SYMBOL (*If applicable*) ASQB-GM	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*) 115 O'Keefe Bldg. Georgia Institute of Technology Atlanta, GA 30332-0800	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO.: 62783A PROJECT NO.: DY10 TASK NO.: 05 WORK UNIT ACCESSION NO.:

11. TITLE (*Include Security Classification*)
MITRE LAD Evaluation

12. PERSONAL AUTHOR(S)
Greg Smith and John Wandelt

13a. TYPE OF REPORT	13b. TIME COVERED FROM_____ TO_____	14. DATE OF REPORT (*Year, Month, Day*)	15. PAGE COUNT
		January 1991	31

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*)

The overall purpose of the evaluation of the MITRE LAD was to identify problem areas for future design efforts. The evaluation focused on three general areas: security, functionality, and administration. Within each of these areas, this document identifies the minimal requirements, describes the implementation methods used by the MITRE LAD to meet these requirements, and presents a comparison between the requirements and the implementation mechanisms.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
[X] UNCLASSIFIED/UNLIMITED [ ] SAME AS RPT. [ ] DTIC USERS	UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (*Include Area Code*)	22c. OFFICE SYMBOL
Michael Evans	(404) 894-3107	ASQB-GM

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

This research was performed for the Army Institute for Research in Management Information, Communications and Computer Science (AIRMICS), the RDTE organization of the U.S. Army Information Systems Engineering Command (USAISEC). This research is not to be construed as an official Army position, unless so designated by other authorized documents. Material included herein is approved for public release, distribution unlimited. Not protected by copyright laws.

THIS REPORT HAS BEEN REVIEWED AND IS APPROVED

s/ James Gantt
James Gantt
Chief, MISD

s/ John R. Mitchell
John R. Mitchell
Director
AIRMICS

DOCUMENT CONTROL NUMBER: A-8752-105

January 15, 1991

MITRE LAD EVALUATION

Contract No. DAKF-11-86-D-15-0030

Prepared for:

DEPARTMENT OF THE ARMY

Headquarters, Forces Command

Ft. McPherson, Georgia 30330-6000

Prepared by:

Greg Smith and John Wandelt

Computer Science and Information Technology Laboratory

Georgia Tech Research Institute

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

LIST OF FIGURES

FIGURE	TITLE	PAGE

FAISS ACCESS TO DODIIS ALTERNATIVES
DCN: A-8752-105; January 15, 1991

1. BACKGROUND

The purpose of this document is to present the results of Georgia Tech Research Institute's (GTRI) evaluation of the MITRE LAD : Local Area Network (LAN) Access to the Department of Defense Intelligent Information System (DODIIS). The MITRE LAD is a prototype development being conducted by MITRE Corporation for the Directorate of Intelligence, J2, Forces Command (FORSCOM) J2.

FORSCOM is interested in the LAD development in order to establish intercommunications and data sharing capabilities between FAISS workstations on a local and global scale. The localized intercommunication requirement is addressed by establishing a local area network where FAISS stations have a centralized file sharing capability. The global intercommunications requirement is addressed by obtaining connectivity to DODIIS through the Defense Intelligence Agency's (DIA) packet switching network, DSNET III. Through DODIIS, non-local FAISS environments can establish a file transfer capability and, in addition, utilize DODIIS as a centralized file storage and retrieval system.

The LAD is primarily intended for fielded operation in a military operational environment. This environmental requirement renders vendor support for the LAD an impracticality. Thus, a LAD operator does not have readily available access to service representatives when problems are encountered. Furthermore, it must be assumed that the LAD operators are military personnel who will possibly have minimal experience and training in computers and network problems. Therefore, the LAD is required to be easy to install and operate, highly reliable, and completely and clearly documented.

2. OBJECTIVES OF EVALUATION

The overall purpose of the GTRI evaluation of the MITRE LAD was to identify problem areas for future design efforts. The evaluation focused on three general areas: security, functionality, and administration. Within each of these areas, this document identifies the minimal requirements, describes the implementation methods used by the MITRE LAD to meet these requirements, and presents a comparison between the requirements and the implementation mechanisms.

Before presenting the evaluation results, a brief description of the MITRE LAD architecture is presented.

3. ARCHITECTURE OVERVIEW

The component level architecture of the MITRE LAD consists of a Novell 2.15 local area network, DOS based FAISS workstations running LANGARD and a DSNET III gateway providing access to DODIIS. At the physical and data link layers, the MITRE LAD is configured as a fiber optic ethernet which is physically connected in a ring topology. The transport and network layers are satisfied by the Transmission Control Protocol (TCP) and Internet Protocol (IP) which execute on the FiberCom/Excelan smart ethernet controller cards. All communications between LAD workstations and the Novell file server utilize either Novell's Internet Packet eXchange (IPX) or Sequenced Packet eXchange (SPX) transport layers on top of TCP/IP. Communications between the attached workstations and the DSNET III gateway utilize the TCP/IP transport. Each workstation, the Novell file server, and the DSNET III gateway are physically and logically directly connected to the ring.

The MITRE LAD allows operation of the FAISS workstations in either network mode or stand-alone mode. In the network mode, a workstation is physically and logically connected to the Novell LAN. In the stand alone mode, the workstation acts independently from the local area network. The stand alone mode is invoked by one of two methods: (1) during the workstation boot process when the network is detected to be unavailable, and (2) when stand alone mode is selected from the menu by the user. Each mode of operation presents its own set of problems and issues.

To perform the LAD evaluation, GTRI setup a LAD system within GTRI facilities. The GTRI LAD was configured as described in the Product Configuration Audit document; GTRI document A-8752-104.

4. MITRE LAD PROTOTYPE SECURITY

4.1 SECURITY REQUIREMENTS

The security requirements for the LAD are directed by FORSCOM and DIA. The FORSCOM directed requirements are concerned with the protection of the FAISS operational data and maintaining the integrity of the workstations; whereas, the DIA directed requirements are focused on providing a protected access to DODIIS.

FORSCOM's requirement for protecting the operational data is two fold. First, the data processed by the system may be classified as high as TS SI/TK and is subject to the appropriate security guidelines. Secondly, the data must be partitioned between system users on a need-to-know basis.

FORSCOM's requirement for maintaining the integrity of the system deals with operational security. The focus of this requirement is to prevent users from inadvertently corrupting or modifying the system software and critical files. At minimum, the users access of the operating system shall be restricted.

DIA serves as the accreditation agency for connectivity to DODIIS. The specific requirements for attaining DIA accreditation for DODIIS connectivity are not readily identifiable. However, DIA accreditation has generally proven to be forthcoming when the potential systems have been designed to approach or meet the requirements established by DOD 5200.28, the "Orange Book", for C2 level security, and the guidelines provided in the National Computer Security Center's (NCSC) "rainbow" series. The minimal subset of the C2 requirements to obtain security accreditation for the LAD are summarized below.

4.1.1 Identification and Authentication

Identification and authentication is directed towards determining if a user is authorized to use the system prior to granting access to any resource under the control of the LAD's security protection system. Each user must be required to utilize a unique password for gaining access to the system. Additionally, users must be restricted from accessing authentication information. [1] The password system must assure authentication of the user's claimed identity, protect against access to the password database, and utilize auditing capabilities to assist in the detection of

password compromise. The password management of the system must insure that default passwords are changed upon system initialization, force users to change passwords on a periodic basis and establish a minimum password length. [2]

4.1.2 Audit

Audit trails are physical records of a system's activity. The C2 requirement for the LAD is to provide audit trails to trace user identification and authentication mechanisms; the creation and deletion of files, the assignment of user accesses, and privileges; any activities of the system administrators and/or system security administrators; all security relevant events; and the production of printed output. The information included in the audits shall minimally include the date and time of the audited event; a unique identification of the user; a description of the event; an indication of the success or failure of event; identification of workstation from which the activity is recorded; the name of any files accessed, added, modified or deleted; and a description of any system administrator modifications to the system configuration. [3]

4.1.3 Discretionary Access Control

Discretionary access control is a means of restricting access to resources and capabilities on a user basis. Discretionary means that the user responsible for a particular resource or capability can allow access by other users at his own discretion. Thus, only authorized users shall have the capability of assigning or changing resource allocations and privileges, and provisions must be made to limit propagation of access rights. Discretionary access control also addresses the problem of object re-use within the system. [4] Object reuse is defined as "the reassignment and reuse of a storage medium ... that once contained one or more objects [programs or data]. To be securely reused and assigned to a new subject [or user], storage media must contain no residual data ...." [5] The implementation of object reuse within the LAD is primarily concerned with the reassignment of Random Access Memory (RAM) and disk storage space within the file server, workstations and gateway. Measurements must be taken to assure that RAM and disk memory are sanitized (i.e., erasure of all previous data) prior to use by a subsequent user, or that RAM and disk memory are physically partitioned to prevent their use as a shared resource.

4.1.4 Assurance Requirements

The assurance requirements are concerned with ensuring that the operation and integrity of the systems protection mechanisms have not been compromised. Minimally, the operation and integrity of the system software shall be protected against external interference or tampering, and procedures shall be established for validating the content and operation of the system software. [6].

4.1.5 Physical Security

The physical construction and integrity of the facility housing the LAN must be in accordance with the principles and criteria set forth in DIAM 50-3. The Sensitive Compartmented Information Facility (SCIF) must be accredited for the highest level of classified material processed by the LAN. Access to the facility should be controlled and implemented to conform to the procedures specified by DIA regulation.

4.1.6 Personnel Security

All computer operators and analysts having physical access to the LAN must possess sufficient clearances. All personnel should be briefed on security procedures and violations. Since the entire LAN is considered system high it is assumed that those having physical access to the LAN will possess the proper clearances. Thus, the focus of the system security mechanisms and internal personnel security procedures is to provide protection and data partitioning on a need-to-know basis.

4.2 SECURITY ARCHITECTURE

In addition to the above mentioned security requirements, there are several security architectural concerns within a local area network. The security architecture employed by the LAN is based on the type of protection mechanisms necessary to guard against anticipated methods of intrusion and violation. Figure 4-1 divides the security of a typical LAN into three areas: file server, LAN/gateway, and workstations. The security architecture employed varies according to the security effort directed towards each of these areas. Typical LAN security architectures are composed of varying measures of the three fundamental approaches to providing LAN security: file server based architecture, workstation based architecture, and LAN/gateway based architecture.

The file server based architecture places all protection mechanisms within the file server(s). This architecture focuses on providing access control and protection to the files and services of the file server. Messages are allowed to propagate within the LAN; however, only authorized users may have access to the file server.

The LAN/gateway based architecture protects against unauthorized access to the LAN and gateway. As shown in Figures 4-2 and 4-3, this architecture requires an additional entity to "police" the LAN and prevent the propagation of unauthorized traffic. This function is performed either by restricting the LAN access (Figure 4-2), or by actually detecting and removing any unauthorized traffic within the LAN (Figure 4-3).

The workstation based security architecture places all the protection mechanisms within the individual workstations. Workstation based architectures protect the workstation from unauthorized access at both the user and the LAN access points. This architecture allows the workstation to monitor, audit, and grant permission to all authorized activity generated by that workstation. The user's access to the LAN, through the workstation, can be restricted with this architecture; however, general access to the LAN and the file server are not protected by the workstation based architecture. For example, Figure 4-4 illustrates that an unprotected workstation can be connected to the LAN allowing unrestrained and unaudited access to the LAN and the file server.

For the LAD to meet the security requirements established in this section, careful design of the security architecture must be employed to prevent weaknesses.

Figure 4-1. - LAN Security Architecture

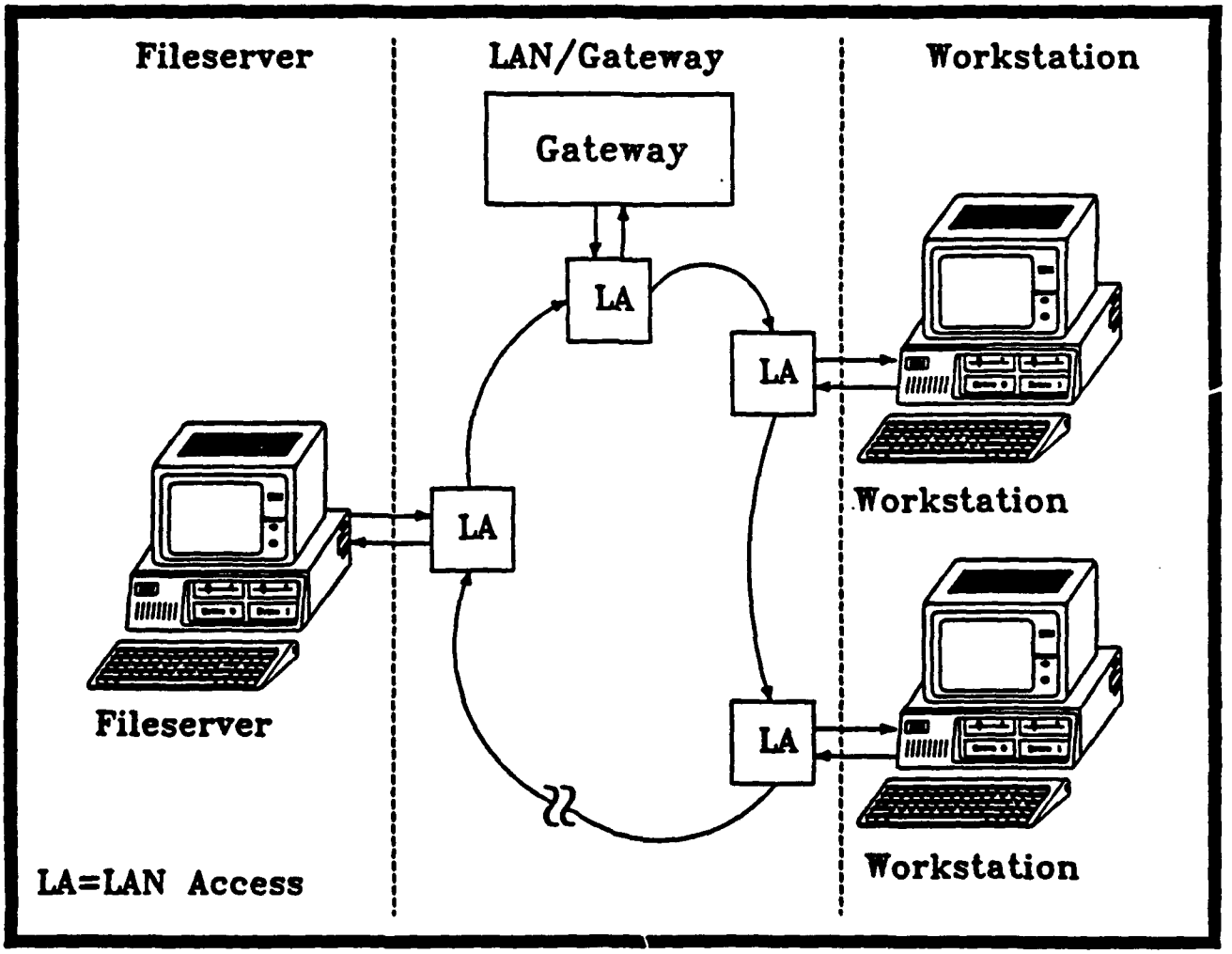


Figure 4-2. - Workstation Access Control to LAN

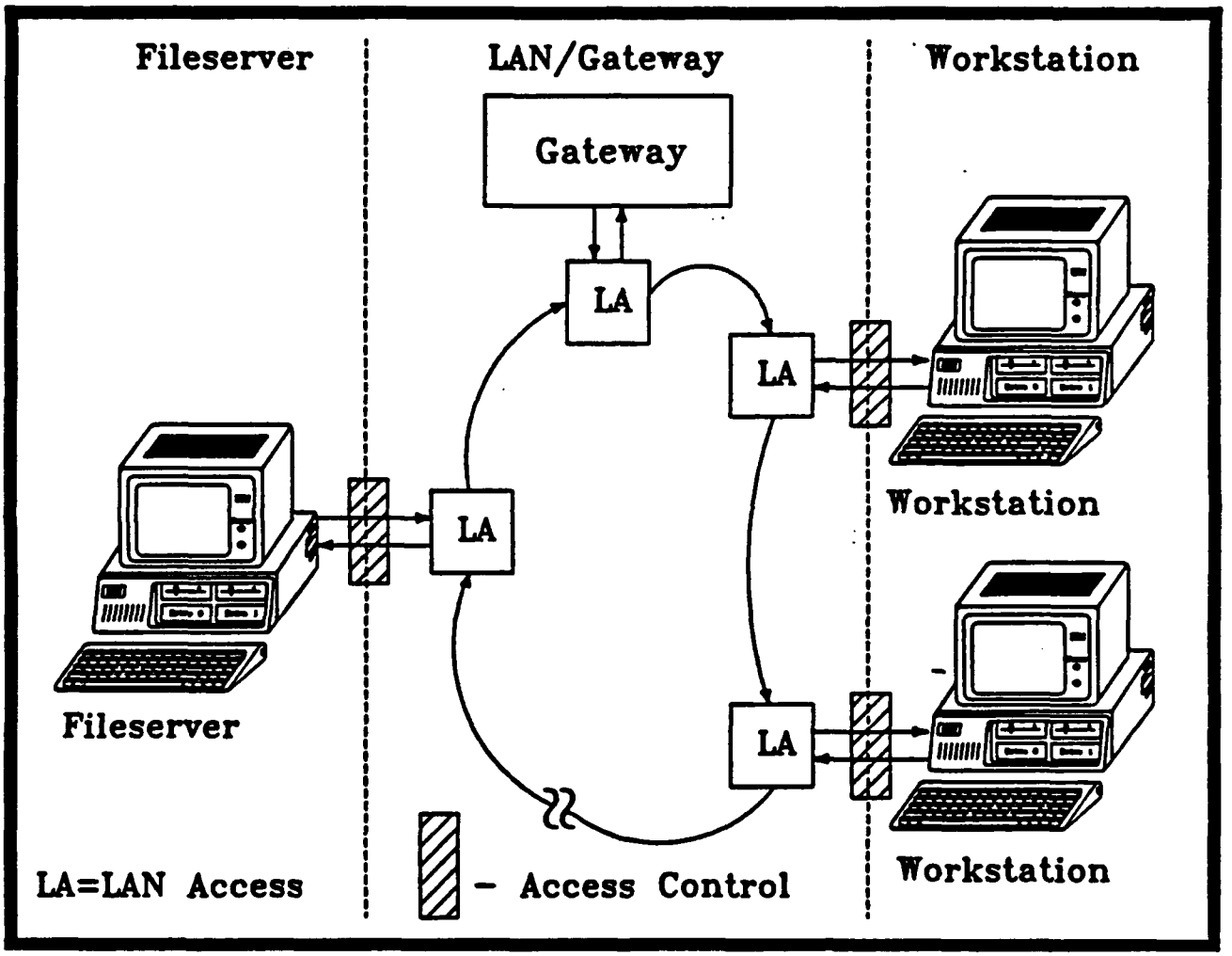


Figure 4-3. - LAN Communications Security Server

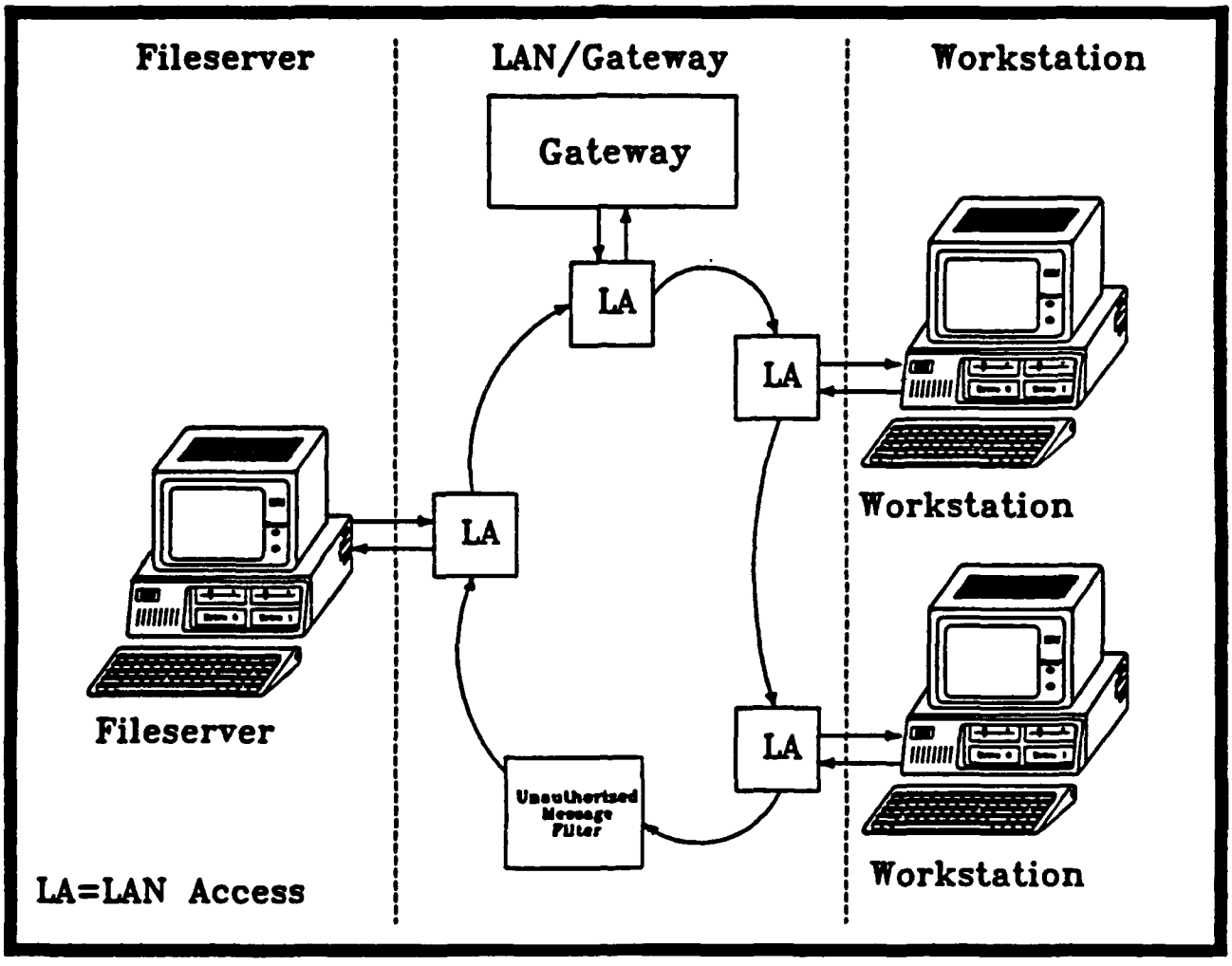
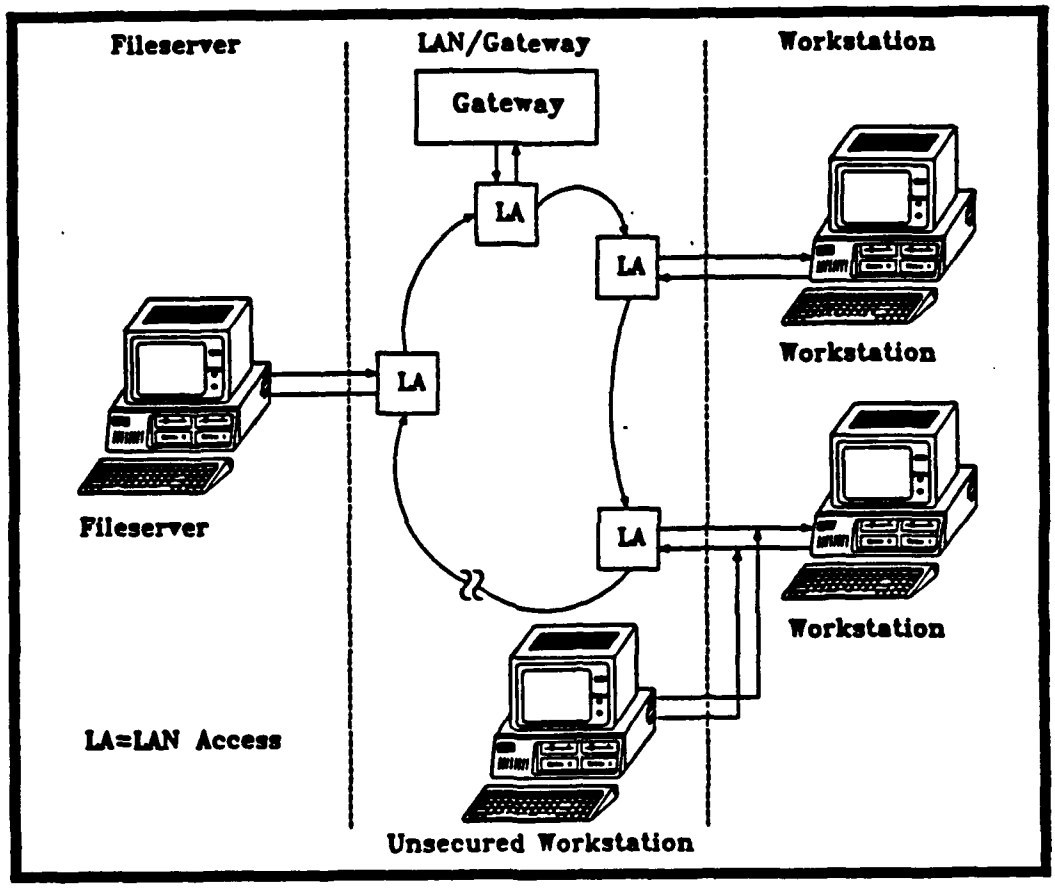


Figure 4-4. - Unauthorized Workstation Insertion



4.3 IMPLEMENTATION MECHANISMS

The MITRE LAD security architecture is composed of four protection mechanisms: (1) LANGARD; (2) procedural/environmental security measures; (3) MITRE custom software and (4) Novell. This section will discuss the role that each of these protection mechanisms has within the MITRE LAD security architecture.

The MITRE LAD primarily utilizes a workstation based security architecture. LANGARD 2.33, the primary protection mechanism employed within the LAD, is a workstation based security package which provides protection to individual workstations operating in a LAN environment. Each workstation within the LAN is configured with the LANGARD protection in both network and stand alone modes of operation. The security features provided by LANGARD fall into three functional areas: access control, command filtering, and boot protection.

LANGARD provides access control to the workstation by use of password protection. The password mechanism with in LANGARD allows the establishment of minimum password lengths, password expiration, system lockout for incorrect login attempts, and timed logoff. In addition, LANGARD provides protection to the workstation and file server programs, directories, files and functions through password protection and menu restrictions.

Once access to the workstation has been granted, LANGARD effectively acts as a command filter by limiting the capabilities of each user through the use of menus. Audit trails are kept on all login attempts and menu item selections. The information included in the audit trails include the selected event, the time and date, the user identification,the workstation identification and files that were operated on.

Finally, LANGARD provides boot protection to the workstation. Boot protection prevents users from by-passing the LANGARD protection by booting the computer from the floppy drive and accessing the files on the fixed drive. It is important to note that the boot protection does not prevent booting from the floppy drive, but rather restricts access to the fixed disk when a workstation has been booted from the floppy drive. The importance of this point will be discussed in the Security Evaluation section.

The procedural/environment security measures employed by the MITRE LAD

include operation of the LAD within a Sensitive Compartmented Information Facility (SCIF). This restriction assures that only TS/SCI/TK cleared users will have access to the LAD. In addition, personnel entering and leaving a SCIF are required to sign a log, thus, allowing an easy determination of the personnel that have had access to the LAD for a specific period of time.

The main security enhancement provided by the MITRE custom software and batch files is the reloading of the system software files from the file server to the workstation during workstation bootup. This process is directed to assuring the integrity of the majority of the system files. The integrity of the file server is assumed. In addition, the MITRE custom software copies all audit trails, collected during workstation stand alone mode, to the file server during the workstation bootup process.

The Novell operating system includes some security functions which are classified as file server based security architecture operations. However, the use of the Novell security functions are optional, and the MITRE LAD does not utilize any of the Novell security functions. Novell's role in the LAD security architecture is to server as a central storage location for security related files such as audit trails.

4.4 SECURITY EVALUATION

A security evaluation can be performed from several perspectives ranging from a friendly user perspective to an internal adversarial perspective. The friendly user perspective looks for security problems that could occur inadvertently; whereas, the internal adversarial perspective assumes that (1) the threat is a person who has access to the system (internal), and (2) is actively attempting to breach the systems security (adversarial). GTRI's security evaluation of the LAD was performed from an internal adversarial perspective. This means that some of the security problems inherent in the LAD may not be applicable to the actual intended use for the LAD; however, it is important to identify these security issues to insure that future use and design efforts with the LAD take these security problems into consideration.

Setting aside the fact that the LAD is operated within a SCIF, the LAD's security architecture is a workstation based security architecture. The workstation based security architecture is ideal for providing protection to workstations; however, this architecture is deficient in providing security protection for the LAN or file server. The only security protection present for the LAN and the file server is the requirement

for SCIF operation. Thus, from the internal adversarial perspective, the LAN and file server are unprotected. The remainder of this section will describe several of the security problems that are inherent to the LAD.

In order to maintain the integrity of the MITRE LAD it is imperative to prevent unrestricted access to the file server. Every workstation reboot process explicitly relies on the integrity of the system files being copied from the file server. If unrestricted access to the file server is obtained, these files could be corrupted and thus effect the integrity of the entire system. Furthermore, since the audit files are stored on the file server, they can be modified.

Unrestricted access to the file server can be accomplished by at least two methods: (1) by attaching an unsecured workstation, equipped with an Excelan card and necessary drivers, to the LAN as previously shown in Figure 4-4; or (2) by booting a workstation from the floppy drive and loading the Excelan and Novell drivers. There are two security gaps which create this vulnerability. The first security gap is that the file server is not configured to require a password for access. The file server is subject to the same identification/authentication requirements as the workstation. The second security gap is that in both of these circumstances, the auditing function of the LAD has been bypassed. This problem exists because the audit of access to the file server is performed by the workstation rather than the file server.

Unrestricted access to the gateway can be obtained in the same manner as unrestricted access to the file server. Similarly, there is no password protection nor auditing capability aside from the workstation's. The security requirements established above clearly indicate that access through the gateway is an event that is subjected to identification and authentication, audit, and discretionary access; however, these requirements are circumvented through the unrestricted access to the gateway.

The MITRE LAD auditing function, besides being vulnerable to bypass, has other security problems. The first problem is that no indication is given as to the result of an audited event (i.e., pass or fail). For example, there is no indication whether an illegal access to the file was successful or prevented. In addition, there is no indication of the success or failure of modifying a users access privileges. This functionality is mandatory in order for the LAD to meet the security requirements established for the C2 security level. The second problem is associated with valid access to the gateway. The MITRE LAD will audit a connection establishment through the gateway; however,

the termination of the connection and establishment of additional connections can occur transparent to the audit function of the LAD. These unaudited connections are established in the following manner:

(1) Establish a valid, audited connection through the LAD's menu selection.

(2) Terminate the connection without exiting the communication package.

(3) Using the communication package command set, establish an invalid, unaudited connection.

Each of these audit problems can be attributed to the security architecture of the MITRE LAD.

The auditing function also has user interface problems. The system administrator should have access to several utilities to assist him/her in examining the audit records. The MITRE LAD implements a filter utility which is intended to allow the system administrator to selectively view records by specifying events, user names, and time frames. However, during the evaluation period, GTRI was unable to successfully use the filter utility. Finally, the audit function should include a report generation utility.

The MITRE LAD password functionally meets the C2 security requirements except for three areas. First, there is no mechanism employed to force the default passwords to be changed upon system installation. This feature could easily be incorporated into the system with the use of LANGARD. Secondly, the system administrator is free to set the minimum password length to one, and the duration of the password validity to infinite. The LAD should contain some mechanism to force the password length and password expiration time to some minimally accepted values. Third, there is no feedback, other than audit trails, that an invalid login attempt is taking place. There should be an audible and visual indicator sent to the system administrator immediately upon this event.

Finally, the download of the system software does not adequately insure the integrity of the system software. The software download utilizes the XCOPY command to copy the system files from the file server to the workstation. The download process does not verify that the files were copied correctly nor does it attempt to verify the integrity of the file server files. A cryptographic checksum on the

system files could have been implemented in order to gain some level of assurance that the file server's files have not been corrupted and that the download was successful.

5. MITRE LAD PROTOTYPE FUNCTIONALITY

5.1 REQUIREMENTS

To meet FORSCOM's operational objectives for the MITRE LAD, several functional requirements must be met. These functional requirements include a local file sharing via a file server, remote login to DODIIS hosts, local and remote electronic mail, local and remote file transfer, and local printer sharing.

The LAD file server must provide a centralized transparent file sharing service to each of the LAN workstations. The file server should have the capability of selectively exporting portions of its disk space. Directories or volumes which contain shared programs and data files should be visible to all necessary workstations simultaneously. This implies that the file server provide application programs with the necessary hooks to perform file and record locking. The file server must also provide the capability of imposing discretionary access restrictions to files, directories, and volumes based on requesting user and/or workstation.

The remote login function is necessary to allow any workstation on the LAD to establish a virtual terminal connection across the DSNET to a DODIIS host. Once the connection is established the workstation should function as if it were directly connected; with the possible exception of time delay for message propagation. It is necessary that LAD workstations are equipped with sufficient terminal emulation capabilities in order to interface with all desired host types. Minimally, the following should be supported: DEC VT100 terminal (TELENT), IBM 3270 (TN3270), and Network Virtual Data Entry Terminal (NVDET). For security considerations it is necessary that all external connections are fully monitored.

Local and remote electronic mail and file transfer functions provide the ability for intercommunication locally between FAISS workstations and globally between FAISS LADs. A standard implementation of these utilities also allows for similar communications between FAISS users and other DODIIS hosts and subscribers. These functions are required to meet the data sharing requirements between FAISS workstations, LAD sites, and the rest of the intelligence community.

Finally, the LAD must provide the functionality of a printer server to support any FAISS generated print output requirements. Space and logistical constraints

imposed by the fielding of a LAD dictate the necessity to share a printer resource.

5.2 IMPLEMENTATION MECHANISMS

The functionality requirements are addressed within the LAD by utilizing several commercial and custom software packages. This section will discuss each of the functional areas that the MITRE LAD design addresses and identify what software packages are utilized in addressing that functional area.

The file server function is provided exclusively through the Novell 2.15 local area network. The Novell LAN and file server provides a centralized file storage and retrieval service. Although the Novell file server has the ability to enforce access restrictions to files and directories, the MITRE LAD uses the LANGARD utility on each workstation to provide this capability. As mentioned earlier, this architecture provides unrestricted and unaudited access to the file server upon bypass of the workstation security. File locking is a service that prevents multiple users from simultaneously accessing and modifying the same file. The LAD does not implement file locking on multiple access files; rather, it depends on application programs such as WordPerfect and FAISS to implement file locking. This is typical, and Novell does provide application programs the necessary hooks to lock a file if necessary.

Remote login and terminal emulation access to DODIIS hosts are implemented by utilizing the DOD standard TELNET protocol on top of TCP/IP. The following terminal emulation packages were selected: Telnet, NVDET, and TN3270. This selection meets the terminal emulation requirements for various types of host systems including, Digital Equipment Corporation VAX and PDP systems as well as IBM systems requiring 3270 terminals.

The local and remote electronic mail capability is not completely addressed by LAD implementation; the capability is limited to a non-standard local delivery only. The local electronic mail function is provided by use of a MITRE customized software program. The MITRE program is basically a file transfer program and operates as follows:

(1) User_1 creates a file with software package A.

(2) User_1 "mails" this file to User_2 with the MITRE mail program.

(3) If User_2 invokes the mail program, he is informed that a file has been received.

(4) User_2 accesses the received file with software package A or some compatible program.

The local file transfer capability for the MITRE LAD is provided either through the local mail facility or indirectly by copying the file from the source workstation to a shared location on the file server and performing a second copy to retrieve the file from the destination workstation. For the remote file transfer capability, the LAD utilizes Excelans implementation of the standard DOD File Transfer Protocol (FTP). The FTP implementation allows both the transfer of ASCII text and binary files. The MITRE LAD is capable of remote file transfer over the DSNET III network with a selective set of hosts. The FTP implementation is a foreground only process, thus the LAD has no capability for performing file transfer as a background process.

The Novell software allows for a print server capability. The LAD documentation did not provide any additional information describing how to take advantage of this capability in a LAD environment.

5.3 FUNCTIONAL EVALUATION

The functional evaluation of the MITRE LAD surfaced several issues that could enhance the LAD. First, it is recognized that the local mail utility for the MITRE LAD was designated as an interim package. However, the deficiencies in the mail utility are included in this section to aid in the design of the final mail utility. Overall, the mail deficiencies can be attributed to the fact that it is in reality, a file transfer utility which, when prompted, notifies a receiver that a message has arrived. In addition to the functional design short comings of the mail utility identified in the evaluation, the successful operation of the mail utility was not observed. After several unsuccessful attempts and consultations to the LAD documentation, it was concluded that the mail utility was not operable. The future design effort in the mail utility should consider the following :

(1) utilizing a standard mail protocol such as the DOD Simple Mail Transfer Protocol (SMTP)

(2) automatic inclusion of headers with each message to allow for message tracing and accountability

(3) an editing function or an interface to an editor or word processor of the user's choice

(4) provision to notify the originator of the mail message that the message has been received and accessed by the receiver

(5) automatic forwarding capabilities, (ie across the DSNET)

(6) a provision for having mail groups

(7) the ability to simultaneously send the message to another party as a carbon copy

The LAD manual advertises a fully monitored access capability to the FAISS LAD by use of a remote PC via an approved communications link (i.e., STU III). However, it is not apparent from the documentation how this connection can be established, if at all. The documentation does not reference any additional hardware requirements for this access, nor does the documentation give an indication of any software support for incoming remote login capabilities.

The remote transfer and terminal emulation functions in the LAD were clear and easy to operate. Minimal input from the user was required and all addressing and protocol issues were transparent to the user. The only problem with the file transfer and terminal emulation packages were that the termination of the current session did not force a return to the user's menu system.

The file and print services implemented by the Novell 2.15 software provided sufficient functionality. These services should have been better integrated into the LAD environment in order to realize their full potential.

6. MITRE LAD PROTOTYPE ADMINISTRATION

6.1 REQUIREMENTS

Evaluation of the administration, management, and maintenance area includes several aspects. First, an examination of the installation procedure is necessary. The criteria for the evaluation is based on the complexity level of the procedure, the user friendliness of the procedure, and the flexibility that the procedure affords to differing system configurations. The complexity level is determined by the amount and type of reading required of the installer; the number of questions and decisions the installer is confronted with; and finally the number of buttons, disks, and manuals that the installer has to manage. The acceptable complexity level of an installation process is dependent upon the environment where the system will be installed, and the training or experience of the installer. For the LAD, the environment should be assumed to be a possible combat environment, and it must be assumed that the installer has a minimum level of training. Therefore, the complexity level of the LAD's installation procedure should be kept to a minimum.

Second, the maintenance procedures and configuration management of the LAD must be examined. The maintenance of the LAD includes the addition, modification, and deletion of resources, whereas, the configuration management includes the addition, modification, and deletion of user accounts. Similar to the installation procedures, the complexity level for the maintenance procedures and configuration management must be at a minimum level.

Third, the security management of the LAD includes the security related aspects of the configuration management, and in addition, includes procedures for isolating security problems, accessing the audit records, and generating usage reports.

Finally, the fault management of the LAD should consist of reporting mechanisms, diagnostic utilites, and procedures necessary to detect and resolve system problems (i.e., resources become unavailable).

6.2 IMPLEMENTATION MECHANISMS

6.2.1 Installation

The installation of the LAD involves four phases: hardware setup, file server installation, system administrator workstation installation, and user workstation installation.

The MITRE LAD delivery consists of software and documentation only. Thus the hardware setup phase requires the user to determine, acquire, and connect the appropriate hardware components. Some of the required hardware components, such as the FiberCom WhisperLAN card and 62.5 micron fiber optic cables, are specified in the documentation, but for the most part the user has the freedom and responsibility for setting up a system which is compatible with the LAD software.

The second phase of the installation consists of configuring the file server and installing the Novell Netware 286 Version 2.15 operating system. This phase is highly user interactive and utilizes the MITRE LAD documentation and the Novell Netware documentation and software.

The third phase consists of installing the system administrator workstation. This process is highly user interactive and utilizes the MITRE software and documentation. The basic procedure consist of loading the system files onto the file server and then copying them to the workstation.

The fourth phase is the installation of user workstations. This phase basically consist of a batch file which copies the appropriate system files from the file server to the workstation.

6.2.2 Maintenance Procedures

The maintenance procedures allowed by the LAD are very limited. Two general categories of resources can be added to a LAN: resources that are attached to and communicate over the LAN, or resources that are accessible through the file server.

The resources accessible through the file server include printers and bridges. These resources are maintained by the Novell software. The resources attached to the LAN are added through use of the MITRE software. The main resources in this category include workstations and gateways. Each resource on the LAN has two

unique addresses: an Ethernet address that is assigned to the LAN interface board, and an Internet Protocol (IP) address that is issued by Defense Communications Agency (DCA). The address-to-name mapping for workstations is accomplished during the initial MITRE software download for each workstation. The address-to-name mapping for external hosts is done through the use of a host file.

6.2.3 Configuration Management

User accounts are added, deleted and modified in the LAD through the use of LANGARD menu selections. The user accounts are accessed by the system administrator through the *SYSTEM MANAGEMENT – USER MAINTENANCE* menu sequence. From the *USER MAINTENANCE* menu, users can be added or deleted, passwords changed, and privileges readjusted.

6.2.4 Security Management

The security management of the LAD is controlled by LANGARD. Selecting the LAD's *USER MAINTENANCE* menu is invokes the LANGARD user maintenance utility. This utility is used to assign passwords parameters such as password level and date of password expiration, and to assign access rights for security related function keys, security switches for overriding system and menu switches, and a directory table to specify the user's directory access rights.

6.3 ADMINISTRATION EVALUATION

The evaluation of the LAD's administration capabilities was written from the perspective that the installer will be a user with minimal computer training who is equipped with LAD compatible hardware and the correct versions of all required hardware and software. This section will present the evaluation of the LAD's installation procedures, maintenance procedures, configuration management, security management, and fault management.

As mentioned in the previous section, the installation of the LAD involves four phases: hardware setup, file server installation, system administrator workstation installation, and user workstation installation. Concerning the hardware setup phase, the LAD documentatoin, gives minimal guidance. Specifications concerning the types of equipment, workstation configurations, and installation and connection of the hardware components are not clearly documented. The hardware setup phase is left to

the user. Even though the LAD deliverable items do not include any hardware components, the user should be provided with clear specifications for the hardware components.

The file server installation procedures were provided through a combination of MITRE documentation and Novell Netware documentation. Overall, the installation procedure was a time consuming and complex process that most likely could not be performed by a user with limited computer training. The installation procedure required too much user interaction and was not clearly documented. During the installation at GTRI, several discrepancies between the installation documentation and the screen prompts were encountered. During the installation process, the user was directed to use the Novell documentation, but was not provided with any page reference, hints, or suggestions. Furthermore, the Novell documentation and procedures were construed to be overly complicated and confusing for a user with minimal computer training.

The file server installation lacked an acceptable level of user friendliness. Several of the user prompts were ambiguous in their meaning and, as mentioned earlier, were not entirely consistent with the documentation. In addition, the installation procedure was unforgiving for input errors and in most instances, did not allow the user to back out or recover from the errors.

Finally, the installation process had a low degree of flexibility concerning differing hardware configurations. For instance, the system that GTRI used as a file server utilized a SCSI hard drive. The effort required to identify, purchase and install the required device driver for this hard drive would have been too complex for an untrained user.

The system administrator workstation installation phase could not be accomplished with the delivered MITRE software. Before installation could commence, the user was required to perform undocumented tasks. First, one of the batch files in the MITRE software had to be modified to include the name of the Novell file server. Secondly, the workstation's hard drive had to be formatted with Compaq MS-DOS 3.31, and the DOS utilities had to be copied onto the hard driver. Once these undocumented procedures were completed, the installation process was straight forward. The system administrator workstation installation procedure included the installation of several application programs onto the workstation. Although including

the application programs in the installation process reduced the amount of effort that was required of the user, there were no mechanisms established to configure the application software for the workstation's configuration.

The general user workstation installation phase was a straight forward process. No problems, were encountered during this phase and the procedure appeared to be performable by a typical user.

To evaluate the maintenance procedures of the MITRE LAD, GTRI chose the task of installing an additional device driver into the system. This task was chosen as an evaluation test because it is one which is often encountered in DOS based environments. The task proved to have no documentation support, and would have been much too complicated for an untrained user. The MITRE batch files actually had to be examined and modified in order to complete the device driver installation. In addition to the results of this test, another maintenance problem was encountered. The problem surfaced during an attempt to remove a workstation from the LAD's available resources. During this procedure, the LAD was placed into an unrecoverable state and ultimately, the file server had to be reinitialized and the Novell operating system and LAD software had to be reloaded. Finally, adding and deleting addresses of available hosts proved to be a cumbersome task. The system administrator was required to invoke a DOS level editor to modify the host tables and routing tables containing the IP addresses.

The configuration management of the LAD, although not well documented, is well designed to for the functions of adding, deleting, and modifying user accounts.

The MITRE LAD did not include any fault management capabilities. Furthermore, the available documentation did not give any indication that fault management is a requirement for the LAD. This shortcoming results in a system that is highly vulnerable. Typical features that should be included in a system such as the LAD are: media backup capabilities for the file server and workstations; detection and notification of unavailable resources; and back up systems for critical functions such as the file server.

7. MITRE LAD PROTOTYPE DOCUMENTATION

The MITRE LAD documentation was incomplete in several areas. One of these areas was the documentation of the specifications for the hardware components. Systems that do not include hardware as a deliverable item are required to give explicit details of the requirements and compatibility problems that exist.

The documentation of the installation phase was not precise and several inconsistencies between the manual and the operation of the system surfaced. The LAD documentation relied heavily on the documentation provided by the commercial packages which comprised the LAD. This is not inherently a disadvantage, although the relationship between the MITRE supplied manuals and other supporting documentation was implied and not explicitly stated. References to non-MITRE documentation were not specific enough to readily facilitate task completion.

8. CONCLUSIONS

The MITRE LAD development was a prototype effort. The purposes of a prototype effort are to identify problem areas associated with the system, weaknesses and strengths inherent to the system design, and alternative approaches to the system design. The outcome of an evaluation should help decide whether future development efforts in the system are practical, cost effective, and technically feasible. The success of the MITRE LAD prototype development supported a thorough system evaluation. The evaluation of the MITRE LAD has uncovered several areas of concern in the system design. This section summarizes the areas of concern and problems that have been presented, and suggests the direction that future effort should take in the development of the LAD.

The foremost area of concern is the LAD's workstation based security architecture. The majority of the security problems presented can be attributed to the security architecture implemented. Any future effort should explore the implementation of a more diversified and distributed security architecture. Aside from a few concerns, the LAD's current security architecture is a good design; however, it needs to be expanded and balanced by including file server and LAN based security architecture characteristics.

The installation procedure of the LAD has several problem areas that must be resolved. The major problem area was the use of Novell 2.15. Functionally, Novell was sufficient for most of the LAD requirements; however, the complexity of the file server installation procedure was entirely unacceptable. Future efforts should either investigate alternatives to Novell 2.15 or investigate the possibility of delivering a pre-configured file sever as part of the LAD's deliverable items.

Several of the problems encountered during the evaluation were hardware related. These problems were, for the most part, due to the use of hardware components which were not directly supported by the LAD software. It is typical for prototype designs to be hard coded and dependent on a specific hardware configuration. The delivered prototype system should have included the hardware components, or at minimum, have included a detailed description of the prototype hardware system. Future efforts in this area need to address compatibility between varying hardware configurations.

Overall, development on the LAD should continue. The prototype phase of the LAD development has demonstrated the technical feasibility of the system, identified several design problem areas that can be addressed and solved, and examined issues related to DIA accreditation for DODIIS connectivity. The next phase of LAD development needs to focus on producing a more portable, robust, and secure product, while achieving a much less complicated procedure for installation and operation.

9. REFERENCES

[1] Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-009, Version-1, pp. 17-20.

[2] Department of Defense Password Management Guideline, CSC-STD-002-85, pp. 4-12.

[3] A Guide To Understanding AUDIT in Trusted Systems, NCSC-TG-001, Version-2, pp. 1,5,9.

[4] Ibid, pp. 20-22.

[5] Glossary of Computer Security Terms, NCSC-TG-004-88, pp. 33.

[6] Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-009, Version-1, pp. 26-29.

10. ACRONYM LIST

ACRONYM	MEANING
ALG	Application Level Gateways
ARPA	Advanced Research Projects Agency
BSD	Berkeley Software Distribution
CGA	Color Graphic Adapter
COTS	Commercial off the Shelf
DEC	Digital Equipment Corporation
DCA	Defense Communications Agency
DCN	Document Control Number
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DIAM	DIA Manual
DODIIS	Department of Defense Intelligence Information System
DSNET3	Defense Secure Network III
EGA	Enhanced Graphics Adapter
FAISS	FORSCOM Automated Intelligence Support System
FCA	Functional Configuration Audit
FCJ2	FORSCOM J2 (Directorate of Intelligence)
FORSCOM	Forces Command
FTP	File Transfer Protocol
GOSIP	Government OSI Profile
GTRI	Georgia Tech Research Institute
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internet Packet eXchange
LAN	Local Area Network
LAD	LAN Access to DODIIS
LPD	Line Printer Daemon
LSO	LAD Security Officer
MAC	Media Access Control
MLS	Multi-Level Secure
MX	Mail eXchange
MIB	Management Information Base
NFS	Network File System
NIC	Network Information Center
NVDET	Network Virtual Data Entry Terminal
OSI	Open Systems Interconnection
POPD	Post Office Protocol Daemon
POSIX	Portable Operating System Interface
PSN	Packet Switched Node

RIPSO	Revised IP Security Option
RFC	Request For Comments
RPC	Remote Procedure Call
SCI	Sensitive Compartmented Information
SA	Systems Administrator
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPX	Sequence Packet eXchange
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VGA	Video Graphics Array
WAN	Wide Area Network
XDR	eXternal Data Representation